Abstract of the Disclosure

A key scheduler for an encryption apparatus using a DES encryption algorithm is disclosed. The key scheduler includes: a first permutation choice unit for permuting a 56-bit block; a first register for storing left 28 bits among the 56-bit block from the first permutation choice unit in accordance with a clock signal; a second register for storing right 28 bits among the 56-bit block from the first permutation choice unit in accordance with the clock signal; a first and a second shift units for shifting the 28-bit blocks stored in the first and the second registers to the left by a first predetermined number of bits and outputting shifted 28-bit blocks to the first and the second registers respectively; a second permutation choice unit for permuting the 28 bits stored in the first and the second registers, thereby generating a first subkey; a third and a fourth shift units, each for shifting the 28 bits stored in the first and the second registers to left by a second predetermined number of bits; and a third permutation choice unit for permuting the 28 bits stored in the third and the fourth shifters, thereby generating a second subkey.